6К

УДК 004.052.03

О.В. Катаев
НИИ многопроцессорных вычислительных систем имени академика А.В. Каляева Южного федерального университета, г. Таганрог, Россия
ovk@mvs.tsure.ru

Об одном подходе к построению отказоустойчивых бортовых многопроцессорных вычислительно-управляющих систем*

В статье предлагается подход к построению бортовых отказоустойчивых вычислительно-управляющих систем, ориентированных на длительные периоды работы без обслуживания. В основу предлагаемого подхода положены концепция построения многопроцессорных вычислительных систем с программируемой архитектурой, разработанная под руководством академика РАН А.В. Каляева, и использование технологии программируемых логических интегральных схем.

Малогабаритные высокопроизводительные высоконадежные вычислительно-управляющие системы, ориентированные на длительные периоды работы без обслуживания, находят широкое применение при создании бортовых управляющих комплексов беспилотных космических аппаратов, автоматических космических станций и спутников, робототехнических комплексов различного назначения и т.п.

Традиционно бортовые вычислительно-управляющие системы строятся с использованием принципов многократного резервирования, что не позволяет получать максимально возможную производительность и приводит к появлению критических (централизованных) ресурсов.

В отличие от известных подходов к построению отказоустойчивых многопроцессорных вычислительно-управляющих систем (МВУС), в основу предлагаемого подхода положены концепция построения многопроцессорных вычислительных систем с программируемой архитектурой (МВС ПА), разработанная под руководством академика РАН А.В. Каляева, и использование технологии программируемых логических интегральных схем (ПЛИС-технологии).

Сочетание концепции МВС ПА и ПЛИС-технологии позволяет осуществлять перестройку архитектуры системы на разных уровнях. На верхнем уровне осуществляется перестройка процессоров и контроллеров системы на определенные операции и изменение топологии связей между элементами системы, на нижнем – изменение конфигурации процессоров (контроллеров) за счет перестройки структуры ПЛИС.

В отличие от известных методов построения отказоустойчивых систем двухуровневая реконфигурация обеспечивает как парирование отказов с использованием резервных ресурсов, так и возможность рационального использования остающегося исправным оборудования и продолжения функционирования системы с деградацией вычислительных ресурсов при значительных нарушениях целостности аппаратно-программных средств.

---

* Работа выполнена при поддержке РФФИ, грант 06-08-00969.

Предлагаются следующие основные принципы построения малогабаритных отказоустойчивых многопроцессорных вычислительно-управляющих систем:

– использование динамической избыточности;
– программное управление избыточностью;
– автономность и однородность базовых модулей МВУС;
– самопроверяемость базовых модулей;
– обеспечение двухуровневой реконфигурации системы.

Основным требованием надежности, предъявляемым к бортовым МВУС, ориентированным на длительные периоды работы без обслуживания, является высокая выживаемость системы на протяжении всего времени функционирования. Это требование трансформируется в высокую вероятность безотказной работы в течение длительного срока (порядка 10^9 часов). Причем довольно часто максимальные требования к вычислительной мощности таких систем предъявляются именно на последних этапах функционирования (например, когда автоматический космический аппарат в конце своего полета встречается с исследуемыми планетами). Как правило, к времени восстановления системы после неисправности (отказа) не предъявляются жесткие требования, однако восстановление должно быть максимально полным с точки зрения выполняемых функций.

Очевидно, что для обеспечения высокой вероятности безотказной работы и полного восстановления необходима достаточно большая избыточность (большое количество резервных базовых модулей) системы. Использование динамической избыточности позволяет обеспечить:

– выживание системы до полного исчерпания резервных базовых модулей (БМ);
– легкость изменения количества резервных базовых модулей (при построении систем, предназначенных для работы в условиях конкретных миссий);
– использование потенциально более низкой интенсивности отказов базовых модулей, находящихся в «холодном» резерве;
– упрощение тестирования основных и резервных БМ (по сравнению со статическим резервированием).

При использовании динамической избыточности целесообразным представляется осуществление программного метода голосования, позволяющего избавиться от критического ресурса (мажоритарного органа).

Структура МВУС представляет собой необходимое количество БМ (в соответствии с требованиями поставленной задачи), объединенных между собой резервированными каналами передачи данных. Для предохранения от катастрофических отказов каждый базовый модуль обеспечивает защиту от распространения неисправностей. Фактически это означает гальваническую развязку каждого БМ от всех остальных компонентов МВУС, а также наличие в каждом базовом модуле своих независимых источников вторичного электроснабжения и генераторов синхросигналов. При этом синхронизация работы всех базовых модулей МВУС осуществляется путем привязки к единому коду бортового времени.

Каждый БМ имеет полный набор программных модулей, которые обеспечивают организацию работы всех бортовых систем космического аппарата, таких как:

– командно-телеметрическая система;
– система ориентации;
– система управления движением;
– система электроснабжения;
– система управления полезной нагрузкой.

Кроме того, в каждом базовом модуле находится программный модуль, выполняющий функции обеспечения отказоустойчивости МВУС. На базовый модуль, выполняющий функции обеспечения отказоустойчивости, возлагаются задачи по организации всей работы МВУС. Чтобы БМ, отвечающий за обеспечение отказоустойчивости МВУС (назовем его «управляющим»), не являлся критическим ресурсом, организуется «теневой» процесс в базовом модуле, функциями которого является резервирование управляющего. Во время межмодульных обменов все БМ обмениваются своими векторами состояний и в случае выхода из строя какого-либо модуля его функции могут быть переданы модулю, находящемуся в резерве. В памяти каждого базового модуля содержится таблица состояния ресурсов системы, где каждый базовый модуль помечается как работающий (и выполняющий определенные функции), резервный или отказавший. В случае обнаружения отказов у «ведомых» или «теневого» базовых модулей «управляющий» БМ исключает их из конфигурации и подключает на их место резервный. В случае отказа «управляющего» БМ выполнение его функций принимает на себя «теневой», который, став «управляющим», тут же вводит в конфигурацию новый «теневой» БМ. Изменение конфигурации системы осуществляется подачей питания на резервные блоки системы и отключение питания от отказавших блоков. После подключения в систему нового БМ он автоматически осуществляет свое самотестирование и в очередном сеансе межмодульных обменов формирует свой вектор состояния. В случае работоспособности подключенного модуля «управляющий» БМ запускает в нем задание, выполняемое отказавшим.

В случае возникновения каких-либо неисправностей в базовых модулях и отсутствия исправных резервных модулей в рабочей конфигурации МВУС может быть использована реконфигурация на нижнем уровне – на уровне программируемых логических интегральных схем (ПЛИС). Для этого необходимо иметь память конфигураций ПЛИС с разными вариантами схемных решений, которые могут обеспечить функционирование базовых модулей с деградацией возможностей. Таким образом, выживаемость системы повышается за счет реконфигурации аппаратно-программных средств на уровне элементной базы.

Процедура выбора начальной конфигурации МВУС обеспечивается последовательным включением базовых модулей. Первый включенный после успешного самотестирования становится «управляющим» модулем, второй – «теневым», третий – принимает на себя выполнение первого задания и т.д.

При наличии неисправных элементов базового модуля решение о выборе выполняемых им заданий принимается на основе анализа вектора состояния аппаратно-программных средств модуля, формируемого по результатам самотестирования. Обмен векторами состояний между всеми БМ системы позволяет сформировать работоспособную конфигурацию МВУС. При этом в каждом БМ находится полная таблица векторов состояния системы.

Сформулируем принципы построения базового модуля бортовой отказоустойчивой МУВС. Каждый базовый модуль должен иметь полный набор аппаратно-программных средств, необходимых для выполнения всех заданий, решаемых МВУС. Ядром базового модуля является ПЛИС, включающая в свой состав процессорные блоки и логические блоки. Кроме того, в состав базового модуля входят:

– источник вторичного электроснабжения;
– генератор синхросигналов;
– оперативная память;

– энергонезависимая память программ;
– энергонезависимая память конфигураций ПЛИС;
– схемы гальванической изоляции модуля.

В ПЛИС формируются устройства, обеспечивающие межмодульный обмен, и устройства, выполняющие сопряжение с различными подсистемами космического аппарата.

В комплексе проблем, возникающих при проектировании малогабаритных отказоустойчивых многопроцессорных вычислительно-управляющих систем (МВУС), своей важностью выделяются проблемы обеспечения своевременного и качественного обнаружения неисправностей (отказов и сбоев) и восстановления вычислительного процесса.

Для минимизации последствий проявления неисправностей в виде разрушения информационной среды вычислительной системы обнаружение ошибок, вызванных неисправностями, должно осуществляться как можно быстрее. Эффективность средств обнаружения ошибок в этом случае будет определяться временем существования необнаруженной ошибки.

С целью создания эффективного комплекса средств обнаружения ошибок (комплекса средств контроля) рассмотрим в общем виде области возникновения потенциальных ошибок в МВУС и методы их обнаружения.

Рассматривая МВУС, можно считать, что системным уровнем возникновения ошибок являются каналы обменов между базовыми модулями и между БМ и другими подсистемами космического аппарата (КА). На уровне БМ источниками ошибок являются элементы памяти (ошибки хранения), устройства преобразования информации (ошибки обработки), устройства формирования последовательности управляющих сигналов (ошибки управления) и каналы передачи информации и регистры (ошибки передачи информации).

Для обнаружения указанных типов ошибок БМ следует применять методы оперативного обнаружения неисправностей, осуществляемые одновременно с нормальной работой базового модуля.

Важным преимуществом оперативного контроля МВУС является то обстоятельство, что он дает возможность быстро приступить к процедуре восстановления нормального функционирования системы. Учитывая, что в качестве основной элементной базы МВУС предлагается использовать программируемые логические интегральные схемы (ПЛИС), которые обладают высокой степенью интеграции эквивалентных логических вентилей и сравнительно низкой стоимостью одного логического вентиля, целесообразным представляется использование следующих основных методов контроля:

– контроль дублированием и сравнением;
– контроль и восстановление ошибок троированием (мажоритарные схемы);
– избыточные коды (контроль по паритету, код Хэмминга).

В настоящее время в бортовой аппаратуре космических аппаратов, ориентированных на длительное функционирование без обслуживания (спутники на околоземной орбите, автоматические космические аппараты в межпланетном полете и т.п.), не используют контроль дублированием и, тем более, троированием на низком уровне (внутри процессорных модулей). Использование ПЛИС позволяет эффективно использовать эти методы оперативного контроля. Дополнить эти методы контроля следует временным контролем – контролем длительности выполнения отдельных функций и

подпрограмм с помощью сторожевых таймеров. Этот контроль позволяет обнаруживать возникновение ошибок по превышению времени выполнения этих функций и подпрограмм.

Средства контроля МВУС могут быть охарактеризованы следующими параметрами, определяющими их эффективность:

– время обнаружения ошибки $T_{обн}$ (время существования необнаруженной ошибки – от момента ее возникновения до момента проявления);

– достоверность контроля $P_{обн}$ (вероятность обнаружения ошибки);

– коэффициент охвата потенциальных ошибок $K_{ох}$ (характеристика полноты покрытия возможных неисправностей);

– объем дополнительных аппаратных средств, обеспечивающих выполнение функций обнаружения ошибок $V_а$;

– объем дополнительных программных средств, обеспечивающих обнаружение ошибок $V_п$.

Оценивание механизмов обнаружения неисправностей в базовых модулях с помощью этих параметров позволит оптимизировать подсистему контроля МВУС. При этом необходимо использовать комплексные критерии оптимизации

$$F_{обн} = \min (T_{обн}, V_а, V_п) \quad \text{и} \quad f_{обн} = \max (K_{обн}, P_{обн}).$$

Появление сигнала об обнаружении ошибки от подсистемы контроля может служить сигналом о необходимости проведения процедуры реконфигурации и восстановления вычислительного процесса в МУВС. Под реконфигурацией МВУС будем понимать восстановление функциональной целостности системы путем замены отказавшего ресурса резервным или восстановление отказавшего ресурса системы.

Замена отказавших базовых (процессорных) модулей при наличии резервных является типичной операцией реконфигурации в отказоустойчивых вычислительно-управляющих системах. Рассмотрим подробнее выполнение реконфигурации МВУС на нижнем уровне.

Возможность перераспределения функций управления, выполняемых различными БМ, связана с наличием в каждом базовом модуле постоянной памяти, хранящей конфигурационные файлы ПЛИС. В этой памяти (внешней по отношению к ПЛИС) хранятся все конфигурационные файлы, которые позволяют каждому БМ выполнять весь набор функций управления системами космического аппарата. Загружая тот или иной конфигурационный файл во внутреннюю оперативную память конфигурации ПЛИС, можно задать те функции управления, которые должен выполнять БМ, в состав аппаратных средств которого входит эта ПЛИС. При выходе из строя отдельных устройств, непосредственно связанных с выполнением определенных функций управления системами космического аппарата (в том числе отдельных выводов или логических блоков самой ПЛИС базового модуля) в ПЛИС можно загрузить другой конфигурационный файл, который позволит работать с имеющимся исправным оборудованием и выполнять другие функции управления. Таким образом, возникает необходимость включения в состав каждого БМ контроллера конфигурации БМ. Задачей этого контроллера является выбор и загрузка во внутреннюю оперативную память конфигурации ПЛИС соответствующего конфигурационного файла из постоянной памяти. Также контроллер конфигурации базового модуля обеспечивает загрузку в оперативную память микропроцессора (микроконтроллера), входящего в

состав БМ, соответствующего программного модуля из постоянной памяти модуля. Эта память хранит все варианты программных модулей, соответствующих вариантам конфигурационных файлов ПЛИС. Кроме того, на контроллер конфигурации можно возложить задачу контроля целостности конфигурационного файла во внутренней памяти ПЛИС и исполняемого программного модуля в оперативной памяти микропроцессора.

Последняя задача связана с тем обстоятельством, что как в оперативной памяти конфигурации ПЛИС, так и в оперативной памяти микропроцессора бортовых космических МВУС под воздействием частиц высоких энергий могут возникать локальные радиационные эффекты (изменение состояния ячейки памяти). Изменение состояния ячеек внутренней конфигурационной памяти ПЛИС, содержащих конфигурационные данные, может привести к изменению структуры устройства, реализованного в ПЛИС, а изменение данных программного модуля, выполняемого микропроцессором, может привести к ошибкам в последовательности выполнения программы (в том числе и «зависанию» микропроцессора). Для того, чтобы избежать подобных ситуаций, контроллер конфигурации периодически должен считывать содержимое внутренней оперативной памяти конфигурации ПЛИС и оперативной памяти микропроцессора и сравнивать эту информацию с соответствующим содержимым постоянных памятей МВУС, хранящих конфигурационные файлы и программные модули. При обнаружении несовпадения контроллер конфигурации должен восстановить информацию во внутренней памяти ПЛИС и в оперативной памяти микропроцессора.

В заключение сформулируем обобщенный алгоритм двухуровневой реконфигурации МВУС.

1. Выполняется нормальное функционирование ПЛИС.

2. Если в БМ возникает сигнал ошибки, то перейти к п. 3, иначе – к п. 1.

3. Выполнить процедуру самотестирования БМ.

4. Если обнаружен отказ БМ, то перейти к п. 5, иначе – к п. 1.

5. Если в МВУС имеются резервные БМ, то перейти к п. 6, иначе – к п. 8.

6. Заменить отказавший БМ резервным. Перейти к п. 1.

7. Проверить приоритет (значимость выполняемой функции) отказавшего БМ. Если приоритет отказавшего базового модуля не является минимальным, то текущему приоритету базового модуля присвоить минимальное значение и перейти к п. 8, иначе – к п. 9.

8. Передать функции отказавшего БМ модулю с минимальным приоритетом.

9. Загрузить в ПЛИС отказавшего БМ конфигурационный файл, соответствующий текущему приоритету.

10. Выполнить процедуру самотестирования БМ.

11. Если БМ работоспособен, то перейти к п. 15, иначе – к п. 12.

12. Проверить, является ли текущий приоритет максимальным. Если является, то перейти к п. 14, иначе – к п. 13.

13. Показатель текущего приоритета увеличить на единицу.

14. Выполнить реконфигурирование МВУС с учетом невозможности полного восстановления функциональной целостности (деградация функциональных возможностей). Перейти к п. 1.

15. Проверить, является ли текущий приоритет минимальным. Если является, то перейти к п. 1, иначе – к п. 16.

16. Передать функции управления, соответствующие текущему приоритету, от работоспособного БМ восстановленному после отказа, а работоспособному – передать функции управления, соответствующие минимальному приоритету. Перейти к п. 1.

Следует отметить, что реконфигурирование с учетом невозможности полного восстановления функциональной целостности МВУС также может быть выполнено на двух уровнях. При этом предполагается, что в постоянной памяти БМ хранятся конфигурационные файлы, заранее учитывающие возможные варианты деградации работоспособности БМ.

Отдельные положения предлагаемого подхода были использованы при проектировании и создании бортовой многопроцессорной вычислительной системы «Аргус», предназначенной для космической программы «Марс 94-96».

О.В. Катаєв
Про один підхід до побудови відмовостійких бортових багатопроцесорних обчислювально-керуючих систем
У статті пропонується підхід до побудови бортових відмовостійких обчислювально-керуючих систем, орієнтованих на тривалий період роботи без обслуговування. В основу запропонованого підходу покладені концепція побудови багатопроцесорних обчислювальних систем з архітектурою, що програмується, яка розроблена під керівництвом академіка РАН А.В. Каляєва, і використання технології логічних інтегральних схем, що програмуються.

O.V. Katayev
In the article is offered a method of design of on-board fault-tolerant computer control systems, intended for long periods of unattended functioning. Method is based on concept of development of multiprocessor computer systems with programmable architecture, worked out under the direction of RAS academician A.V. Kaliaev, and on FPGA-technology.

Статья поступила в редакцию 25.06.2008.